TIN: Terapan Informatika Nusantara
Vol 4, No 11, April 2024, page 698-708
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v4i11.5060

Analisis Keamanan Website Pendaftaran Mahasiswa Baru Dengan Munggunakan Metode Vulnerability Assessment

Sherli Ameilia Hafsari, Harjono*

Fakultas Teknik dan Sains, Program Studi Teknik Informatika, Universitas Muhammadiyah Purwokerto, Purwokerto, Indonesia
Email: [1]Sherliameliah@gmail.com, [2*] harjono@ump.ac.id
Email Penulis Korespondensi: harjono@ump.ac.id

Abstrak−*Website* memegang peran penting dalam konteks pendidikan, seperti dalam pengelolaan sistem akademik, penerimaan mahasiswa baru, serta fungsi lainnya. Publikasi yang dilakukan secara online dengan memanfaatkan *website* resmi kampus dapat mempermudah orang tua ataupun pendaftar mahasiswa dari daerah luar kota atau bahkan luar pulau bisa mencari informasi lengkap seputar perguruan tinggi yang diinginkan. Universitas Muhammadiyah Purwokerto terdapat sistim pendaftaran mahasiswa baru secara online melalui sebuah website pmb.ump.ac.id. Suatu instansi atau organisasi dapat mengalami kerugian jika informasi yang didapatkan jatuh kepada pihak yang tidak berwenang, sehingga sebuah sistem informasi harus memiliki kemampuan untuk mengatasi dan menghentikan langkah-langkah buruk yang diinginkan. Untuk mencegah kejadian tersebut maka penelitian ini diterapkan dengan menggunakan metode *Vulnerability Assessment* dengan tujuan untuk mandapatkan informasi celah keamanan dan kerentanan pada website pendaftaran mahasiswa baru Universitas Muhammadiyah Purwokerto. Hasil pengujian yang diperoleh dengan menggunakan alat *vulnerability* ditemukannya sejumlah celah keamanan pada *website* pendaftaran mahasiswa baru Universitas Muhammadiyah Purwokerto. Peneliti telah memberikan beberapa rekomendasi untuk mengatasi terkait temuan celah keamanan yang dapat digunakan.

Kata Kunci: Website; Mahasiswa Baru; Online; Sistem Informasi; Vulnerbality Assessment

Abstract−The website plays an important role in the educational context, such as in managing the academic system, accepting new students, and other functions. Publications carried out online by utilizing the official campus website can make it easier for parents or student registrants from areas outside the city or even outside the island to find complete information about the desired university. Universitas Muhammadiyah Purwokerto has an online student registration system through a pmb.ump.ac.id website. An agency or organization can suffer losses if the information obtained falls to unauthorized parties, so an information system must have the ability to overcome and stop the desired bad steps. To prevent these events, this research was applied using the Vulnerability Assessment method with the aim of obtaining information on security gaps and vulnerabilities on the new student registration website of Universitas Muhammadiyah Purwokerto. The test results obtained using the vulnerability tool found a number of security holes on the new student registration website of the University of Muhammadiyah Purwokerto. Researchers have provided several recommendations to address the findings of security holes that can be used.

Keywords: Website; Freshman; Online; Information System; Vulnerability Assessment

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini berkembang dengan pesat(Purba et al., 2021). Terutama teknologi internet(Luthfansa & Rosiani, 2021). Internet adalah sebuah teknologi yang terus berkembang, dan terus dikenal serta digunakan banyak orang(Maharani et al., 2021). Interconnection networking, juga dikenal sebagai Internet adalah semua jaringan komputer yang saling terhubung menggunakan Protokol Pengendalian Transmisi/Paket Protokol Internet (TCP/IP), yang merupakan protokol pertukaran paket atau protokol komunikasi paket. Internet melayani miliaran pengguna di seluruh dunia(Hansen & Panggabean, 2023). Pada tahun 1990 pertama kali sejarah internet dikenal di Indonesia(Sunanta & Wulandari, 2023). Keberadaan teknologi informasi seperti internet telah memungkinkan kita memandang secara global, berinteraksi dan *marketplace* baru, hingga jaringan bisnis tanpa batas(Lestari et al., 2022). Dunia dalam internet atau era digital ini disebut dunia maya atau *cyberspace*(Keriapy et al., 2022). Kehadiran internet sebagai infrastruktur dan jaringan telah meningkatkan efektivitas dan efisiensi operasional perusahaan, terutama dalam fungsi sebagai alat publikasi, komunikasi, dan sumber informasi yang penting. Informasi di internet biasanya dipublikasikan melalui situs web yang dibuat menggunakan bahasa pemrograman HTML (*Hypertext Markup Languange*)(Alcianno, 2020).

Website adalah kumpulan halaman yang saling terhubung yang di dalamnya terdapat beberapa item seperti dokumen dan gambar yang tersimpan di dalam web server(Iin Nuraeniah, Muhamad Fatchan, 2024). Kemunculan media online ditandai dengan adanya *World Wide Web* (WWW) yang diciptakan oleh Tim Berners Lee pada tahun 1989(Kustiawan et al., 2022). Semuanya dimulai ketika dia berhasil menemukan suatu cara untuk menghubungkan atau mengaitkan dokumen satu dengan yang lain di internet, dan website merupakan hasil evolusi dari metode ini. Pada tahun 2000, Tim O'Reilly pertama kali mengusulkan konsep Web 1.0, dan Web miliknya populer karena semua perusahaan mulai memanfaatkan media ini untuk mengembangkan bisnisnya. Di zaman serba cepat ini, *website* juga menjadi salah satu tempat terjadinya kesepakatan antara penjual dan pembeli, atau yang lebih dikenal dengan sebutan *ECommerce*(Firmansyah & Herman, 2023). *Website* juga berperan penting dalam pendidikan karena menjadi salah satu media publikasi resmi bagi sebuah instansi. *Website* sebagai sarana informasi yang lebih mudah dan cepat untuk didapatkan(Ushud et al., 2021). Salah satu instansi yang seharusnya memiliki situs web ialah perguruan tinggi. *Website* memegang peran penting dalam konteks pendidikan, seperti dalam pengelolaan sistem akademik, penerimaan mahasiswa baru, serta fungsi lainnya(Hasanah, 2020). Publikasi yang dilakukan secara online dengan memanfaatkan

TIN: Terapan Informatika Nusantara
Vol 4, No 11, April 2024, page 698-708
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v4i11.5060

website resmi kampus dapat mempermudah orang tua ataupun pendaftar mahasiswa dari daerah luar kota atau bahkan luar pulau bisa mencari informasi lengkap seputar perguruan tinggi yang diinginkan. Universitas Muhammadiyah Purwokerto terdapat sistim pendaftaran mahasiswa baru secara online melalui sebuah website pmb.ump.ac.id. Website pendaftaran mahasiswa baru pada Universitas Muhammadiyah Purwokerto merupakan sebuah inovasi yang memudahkan dalam penerimaan mahasiswa baru dimana memiliki layanan yaitu calon mahasiswa dapat mendaftar langsung secara online melalui website tersebut tanpa harus datang ke instansi terkait.

Bersama dengan kemajuan teknologi dan ketergantungan pada *platform online*, pentingnya keamanan situs web semakin meningkat(Syafaat & Subang, 2024). Indonesia juga menghadapi tantangan global terkait dengan keamanan dan ketahanan nasional di dunia maya(Aulianisa & Indirwan, 2020). Menurut laporan tahunan yang dirilis oleh Id-SIRTII/CC dan Badan Siber dan Sandi Negara melalui Lanskap Keamanan Siber Indonesia 2022, keseluruhan jumlah anomali di Indonesia selama tahun 2022 mencapai total 976.429.996 kejanggalan yang terdeteksi. Sedangkan kasus web defacement di Indonesia pada tahun 2021 mencapai 5.940 kasus dan pada tahun 2022 sebanyak 2.348 kasus *Web Defacement* yang terjadi di Indonesia(Badan Siber dan Sandi Negara, 2022). *Web defacement* merupakan salah satu celah keamanan yang dimanfaatkan oleh seseorang untuk menyerang sebuah website(Kestina & Nurcahyo, 2023). Keamanan *cyber* telah menjadi isu prioritas seluruh negara di dunia semenjak teknologi informasi dan komunikasi dimanfaatkan. Sejalan dengan peningkatan penggunaan teknologi informasi dan komunikasi, tingkat risiko dan ancaman penyalahgunaannya juga meningkat secara signifikan dan menjadi lebih kompleks(Siber & Sandi, 2022). Keamanan data dalam sistem informasi akademik menjadi kritis dalam era digital saat ini(Saputra et al., 2024). Oleh sebab itu perlu adanya analisis terhadap celah keamanan pada sistem informasi pmb.ump.ac.id. Menurut (Adawiyyah et al., 2023) bahwa keamanan informasi adalah upaya untuk memastikan dan menjamin kelangsungan bisnis dengan melindungi informasi dari berbagai ancaman untuk mengurangi risiko dan memaksimalkan peluang bisnis.

Suatu instansi atau organisasi dapat mengalami kerugian jika informasi yang didapatkan jatuh kepada pihak yang tidak berwenang, sehingga sebuah sistem informasi harus mampu memiliki kemampuan mengatasi dan menghentikan langkah-langkah buruk yang diinginkan. Setiap instansi harus memperhatikan keamanan informasi sebagai suatu keharusan, untuk menghindari gangguan atau aktivitas kejahatan. Kurangnya pemahaman dan kesadaran terhadap keamanan sistem dapat menjadi ancaman terutama bagi para pengembang. Seiring berjalannya waktu bertambahnya sumber daya manusia, kebocoran atau perusakan data dapat terjadi kapan saja. Masalah keamanan atau gangguan tersebut bisa berupa seranagan *Malware, Cross Site Scripting (XSS), Injeksi Database* dan laim sebagainya.

Sejumlah peneliti menyatakan bahwa untuk mengidentifikasi celah keamanan pada suatu sistem *website* dapat dengan metode *vulnerability assessment.* Hal ini dibuktikan oleh (Wahyudin et al., 2024) telah melakukan metode *vulnerability assessment* dalam pengujian kinerja sistem keamanan *website points of sales*. Dalam penelitian ini melakukan *vulnerabilities scanning* dengan menggunakan nikto yang dijalankan melalui OS/*system* Kali Linux dan owasp zap. Berdasarkan proses pengujian yang telah dilakukan, terdapat ada banyak sekali *ports* yang terbuka serta *service* yang berjalan, dari proses pengujian juga diketahui level kerentanan website sakupos.com, dari masing-masing *tools* tidak ada *tools* yang paling handal namun masing-masing *tools* saling melengkapi untuk menjelaskan kerentanan dalam *website*. Disamping itu, ada penelitian yang dilakukan oleh (Harahap & Zufria, 2024) juga menggunakan metode *vulnerability assessment* terhadap *website* UPM Saintek UIN-SU Medan. Penelitian tersebut melakukan analisis keamanan terhadap website UPM SAINTEK UIN-SU Medan dengan menggunakan metode vulnerability assessment, dan dari proses ini berbagai kerentanan ditemukan dengan menggunakan alat owasp zap dan open vas. Hasil tersebut mengungkapkan tingkat resiko keamanan yang dapat dieksploitasi oleh pihak lain, dan memberikan pemahaman mendalam tentang kondisi keamanan tersebut. Selain itu penelitian yang dilakukan oleh (Taryana & Nono, 2023) berjudul analisis keamanan *website* BPJS Kesehatan menggunakan metode *vulnerability assessment*. Aplikasi yang digunakan pada penelitian tersebut yaitu owasp zap, hasil pengujian yang diperoleh, telah ditemukan 11 celah kerentanan pada *website* BPJS Kesehatan yang dipaparkan dengan owasp zap versi 2.11.0 kemudian diperoleh solusi untuk menangani kerentanan pada *website* tersebut. Penelitian yang dilakukan oleh (Laksmiati, 2023) mengidentifikasi kerentanan pada situs web berbasis WordPress www.mobilemuslim.id menggunakan metode *vulnerability assessment*. Pada penelitian tersebut situs web memeliki kerentanan yang diidentifikasi menggunakan NMAP dan WPScan. Temuan NMAP terutama berkaitan dengan konfigurasi fitur. Penelitian yang dilakukan oleh (Muharrom & Saktiansyah, 2023) menggunakan metode *vulnerability assessment* dengan OpenVas pada jaringan PT.Dutakom Wibawa. Penerapan Teknik *vulnerability assessment* menggunakan OpenVas pada PT. Dutakom Wibawa Putra network telah memberikan wawasan mengenai keamanan infrastruktur jaringan perushaan namun, penting untuk mengakui keterbatasan tertentu dari penelitian tersebut dan menyarankan arah untuk penelitian dimasa depan. Efektivitas *vulnerability assessment* menggunakan OpenVas dapat bervariasi tergantung pada lingkungan dan konfigurasi jaringan tertentu. Studi ini berfokus pada kasus tertentu, dan hasilnya mungkin tidak langsung berlaku untuk semua scenario. Penelitian yang dilakukan oleh (Riadi et al., 2020) mengenai keamanan untuk *website open journal system* dengan metode yaitu *vunerability assessment*. Objek penelitian tersebut mencari *vulnerability* dalam struktur *file*, server web *Open Journal System*(OJS) mencakup sistem yang dikelola oleh *admin* dengan menggunakan tools owasp. Kelebihan dari *tool* owasp dapat melihat *source* code yang ditandai kusus oleh *tool* owasp. Owasp berhasil menguji kerentanan sistem ojs, telah ditemukan 3 tingkat kerentanan, yitu *high, medium* dan *low*. Penelitian yang dilaksanakan oleh (Prasetya, 2023) menerapkan metode vulnerability assessment pada situs web perpustakaan SMAN 3 Tambun Selatan. Pada tahapan *vulnerability* pengujian website perpustakaan SMAN 3 Tambun Selatan dilakukan menggunakan tool owasp zap. Berdasarkan pengujian dengan menggunakan alat owasp zap ditemukan 8 *alert.* Dari beberapa penelitian yang telah

TIN: Terapan Informatika Nusantara
Vol 4, No 11, April 2024, page 698-708
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v4i11.5060

dilakukan oleh para peneliti tersebut untuk mengetahui kerentanan dan celah keamanan pada sebuah *website* dengan metode *vulnerability assessment* mereka menggunakan lebih dari satu *tools vulnerbality assessment* untuk *website*, terdapat banyak *website* yang telah berhasil ditemukannya celah keamanan dengan melakukan *vulnerability scanning* menggunkana tools *vulnerability scanning.* Owasp Zap merupakan alat yang banyak digunakan oleh para peneliti buat melakukan *vulnerability assessment* terhadap *website* dengan kelebihan dapat melihat *sorce code* yang ditandai kusus oleh *tool* owasp serta memberikan pemahaman mendalam tentang kondisi keamanan *website.* Hal ini dapat disimpulkan bahwa metode *vurnerability assessment* dapat mengidentifikasi, mengevaluasi, dan mengurangi kerentanan atau celah keamanan pada aplikasi berbasis *website.*

Vulnerability assessment adalah proses mendefinisikan, mengidentifikasi, dan menempatkan kerentanan dalam sistem komputer, aplikasi, dan struktur jaringan secara berurutan. Proses ini menyediakan organisasi dengan evaluasi yang diperlengkapi dengan pemahaman, kesadaran, dan konteks risiko yang diperlukan untuk mengerti ancaman terhadap lingkungannya dan bertindak sesuai. Alat uji otomatis seperti pemindaian keamanan jaringan biasanya digunakan dalam proses evaluasi kelemahan untuk mengidentifikasi ancaman dan risiko yang ditimbulkannya. Hasil evaluasi kelemahan didokumentasikan dalam laporan evaluasi kelemahan.(Rohim & Setiyani, 2023).

Berdasarkan latar belakang yang telah dijabarkan, maka dilakukan penelitian ini dengan tujuan untuk mandapatkan informasi celah keamanan dan kerentanan pada *website* pendaftaran mahasiswa baru Universitas Muhammadiyah Purwokerto.

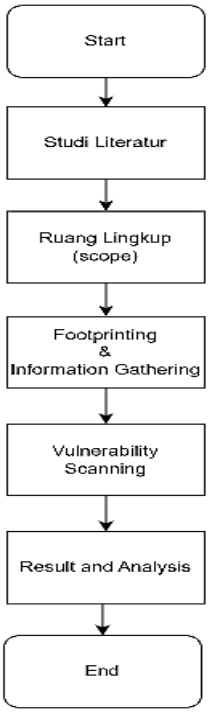
2. METODE PENELITIAN

2.1 Kerangka Dasar Penelitian

Penulis menggunakan penelitian jenis kualitatif. Penelitian kualitatif adalah penelitian yang berfokus pada deskripsi dan biasanya melibatkan analisis. Pada penelitian kualitatif cenderung menekankan proses dan makna. Penelitian ini diterapkan dengan menggunakan metode *vulnerability assessment.* Metode *vulnerability assessment* merupakan metode untuk mengidentifikasi beberapa kerentanan dalam situs web dan menyarankan cara untuk memperbaikinya. Fokkus dari penelitian ini adalah situs web pendaftaran *online* calon mahasiswa baru di Universitas Muhammadiyah Purwokerto dengan pengujian kerentanan akan dilakukan dengan memanfaatkan alat dan aplikasi pemindai kerentanan guna mengidentifikasi informasi tentang kerentanan yang ada.

2.2 Tahapan Pada Penelitian

Tahapan atau langkah-langkah adalah rangkaian tindakan atau prosedur dalam rangka merencanakan, melaksanakan, dan mengevaluasi sebuah penelitan. Tahapan-tahapan ini membantu peneliti untuk menjalankan penelitiannya secara sistematis dan efektif. Adapun tahapan-tahapan penelitian yaitu studi leteratur, ruang lingkup (scope), *footprinting and Information gathering, vulnerability scanning, result and analysis.* Berdasarkan studi diatas, maka tahapan dalam penelitian digambarkan seperti dibawah ini:



Gambar 1. Tahapan Penelitian

TIN: Terapan Informatika Nusantara
Vol 4, No 11, April 2024, page 698-708
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v4i11.5060

Tahapan-tahapan penelitian:

a. *Studi Literatur*
   Peneliti mengumpulkan data dan informasi sebanyak-banyak nya, guna mencapai hasil penelitian yang objektif.
b. Ruang Lingkup (*scope)*
   Peneliti menentukan batasan-batasan (*scope*) terhadap *website* pmb.ump.ac.id yang hanya melakukan pemidaian kerentanan secara pasif tanpa melakuakan pengeksploitasi terhadap sistem seperti mengubah tampilan, melakukan serangan DdoS, dan sebagainya.
c. *Footprinting and Information Gathering*
   Merupakan langkah untuk memeperoleh data informasi perangkat jaringan.
d. *Vulnerability Scanning*
   Pada tahap ini peneliti melakukan pemindaian kerentanan dengan memanfaatkan berbagai alat pemindai kerentanan (seperti acunetix, owasp zap, dan nikto). *vulnerability scanning* dengan menggunakan berbagai *tools vulnerability scannin* (Acunetix, OWASP ZAP, dan Nikto). Tujuannya adalah untuk menemukan kerentanan keamanan pada situs web, serta mencangkup *SQL Injection, Cross Site* (XSS) *Remote OS Command Path Transversal* pada sistem pmb.ump.ac.id.
e. *Result and Anallysis*
   Menyajikan hasil analisis mengenai kerentanan keamanan yang terdeteksi oleh peneliti dan saran solusi.

Dalam melakukan penelitian dengan metode *vulnerability assessment*, beberapa alat atau *tools* menjadi kunci untuk mengidentifikasi potensi kerentanan dalam sistem yang diteliti. Berikut adalah alat yang digunakan dalam *vulnerability assessment*:

Tabel 1. *Tools Footprinting and Information Gathering, Vulnerability Scanning*

No	*Tools*	Fungsi
1.	Zenmap	Aplikasi sumber terbuka untuk mengeksplorasi jaringan dan audit keamanan.
2.	Acunetix	Aplikasi tersebut dapat mencari dan memberitahukan berbagai jenis kerentanan dalam aplikasi yang dikembangkan di berbagai platform seperti *WordPress, PHP, ASP NET, Java Frameworks, Ruby on rails* dan sebagainya.
3.	Dnsdumpster	Aplikasi yang dapat menghimpun informasi dan memetakan domain serta subdomain tertentu.
4.	OWASP ZAP	Aplikasi pentest digunakan untuk mengidentifikasi kerentanan dalam aplikasi web.
5.	Nikto	Alat pemindaian aplikasi web yang mencari kesalahan konfigurasi direktori yang dapat diakses secara terbuka dan berbagai kerentanan pada aplikasi web.

2.3 *Website*

Website atau situs adalah sekumpulan halaman dipergunakan untuk menampilkan berbagai informasi dalam bentuk teks, gambar, animasi, suara, dan juga kombinasi dari semua itu. Halaman-halaman tersebut dapat bersifat statis atau dinamis, membentuk suatu struktur terkait yang saling terhubung dan dapat diakses melalui jaringan.(Karyati, 2024).

2.4 Keamanan *Website*

Keamanan *website* merupakan hal penting untuk mencegah berbagai upaya jahat yang dapat merugikan bisnis secara digital, serta untuk mencegah akses ilegal dan penggunaan informasi pribadi yang tersedia di situs web. Penting untuk secara rutin memeriksa keamanan situs web guna mendeteksi kesalahan atau celah dalam keamanannya.(Saraswati et al., 2024).

2.5 Metode *Vulnerability Assessment*

Penilaian kerentanan, atau *vulnerability assessment*, merupakan metode yang digunakan untuk menguji titik-titik yang rentan terhadap serangan potensial, termasuk port-port yang terbuka, identifikasi perangkat lunak, serta aplikasi yang sedang beroperasi. Tujuannya adalah untuk mendeteksi kelemahan dalam sistem yang ada(Rizkayanti & Yunanri, 2023).

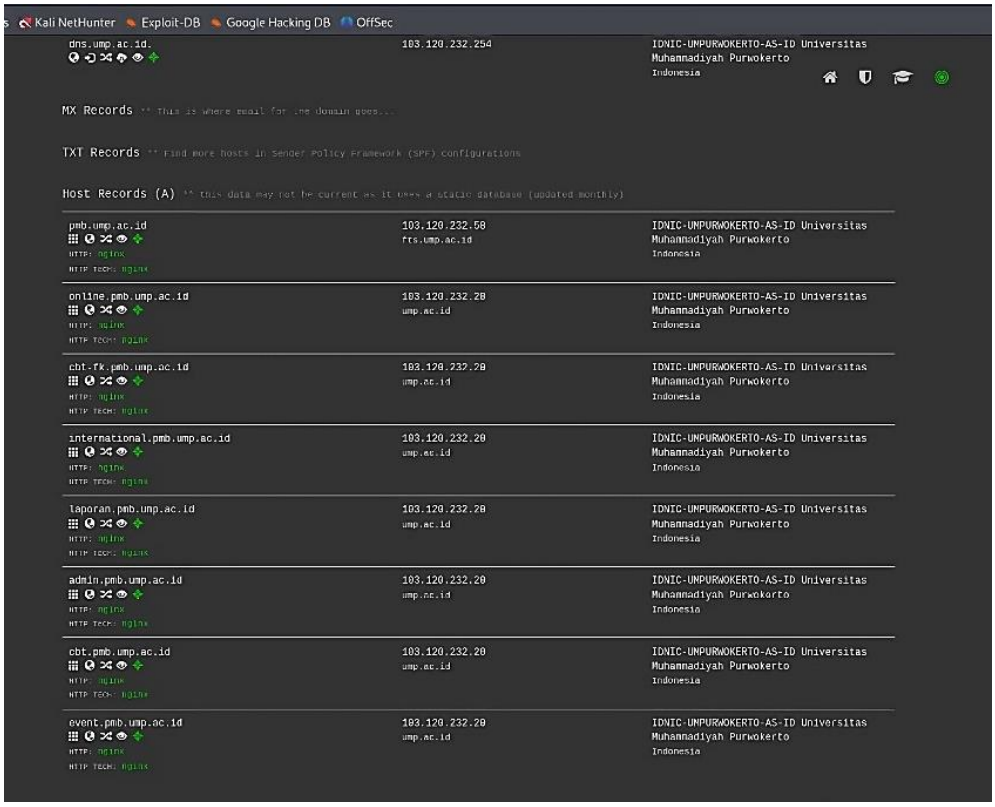
3. HASIL DAN PEMBAHASAN

3.1 *Result and Analysis*

3.1.1 Pengujian *footprinting* dan *information gathering*

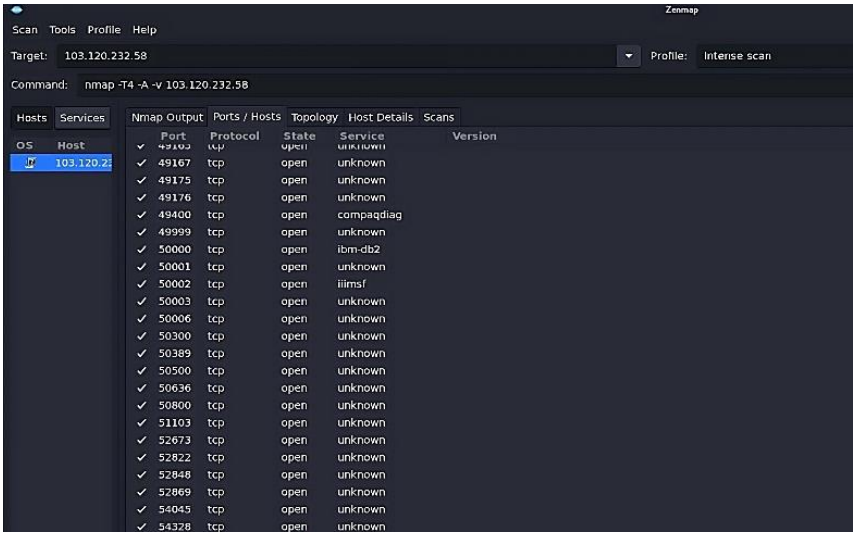
Pada tahapan ini penulis mengumpulkan informasi dari situs web pendaftaran mahasiswa baru Universitas Muhammadiyah Purwokerto. Penulis menggunakan *tools* DNSDumpster, DNSDumpster adalah alat *online* yang digunakan untuk melakukan pemindaian DNS terhadap suatu domain. Alat ini memungkinkan pengguna untuk mendapatkan informasi penting tentang infrastruktur jaringan terkait dengan domain yang diteliti. Proses *scanning* dengan DNSDumpster terlihat pada gambar 2 dibawah ini:

TIN: Terapan Informatika Nusantara
Vol 4, No 11, April 2024, page 698-708
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v4i11.5060



Gambar 2. *Scanning* DNSDumpster

Dengan menggunakan layanan DNSDumpster ini memungkinkan peneliti untuk memeriksa dan memperoleh informasi DNS terkait dengna suatu domain tertentu. Dalam *scanning* DNSDumpster ini digunakan untuk memperoleh informasi ip server yang akan digunakan pada tahap selanjutnya. Setelah melakukan *scanning* dengan DNSDumpster dan memeperoleh infomormasi, maka dilakukan *scanning* menggunakan zenmap untuk memperoleh informasi jaringan. Zenmap merupakan sebuah antarmuka grafis yang dirancang untuk Nmap, yang merupakan sebuah utilitas jaringan yang kuat dan sering digunakan dalam bidang keamanan komputer dan administrasi jaringan. Zenmap menyediakan antarmuka pengguna grafis (GUI) untuk Nmap, yang mempermudah pengguna dan interpretasi hasil pemindaian jaringan. Proses *scanning* dengan Zenmap dapat dilahat pada gambar 3 dibawah ini:



Gambar 3. *Scanning* zenmap

Pada *scanning* zenmap memperoleh pemindaian jaringan dan visuali data. Dari hasil pada gambar 3 diatas menunjukkan bahwa *scanning* terhadap IP Server website dengan perintah command nmap-T4 -A -v 103.120.232.58.

3.1.2 Hasil pengujian *footprinting* dan *information gathering*

Setelah melakukan pengujian dengan *scanning* dnsdumpster dan *scanning* zenmap menemukan beberapa informasi terkait jaringan website pmb.ump.ac.id yang dapat dilihat pada Tabel 2 dibawah ini:

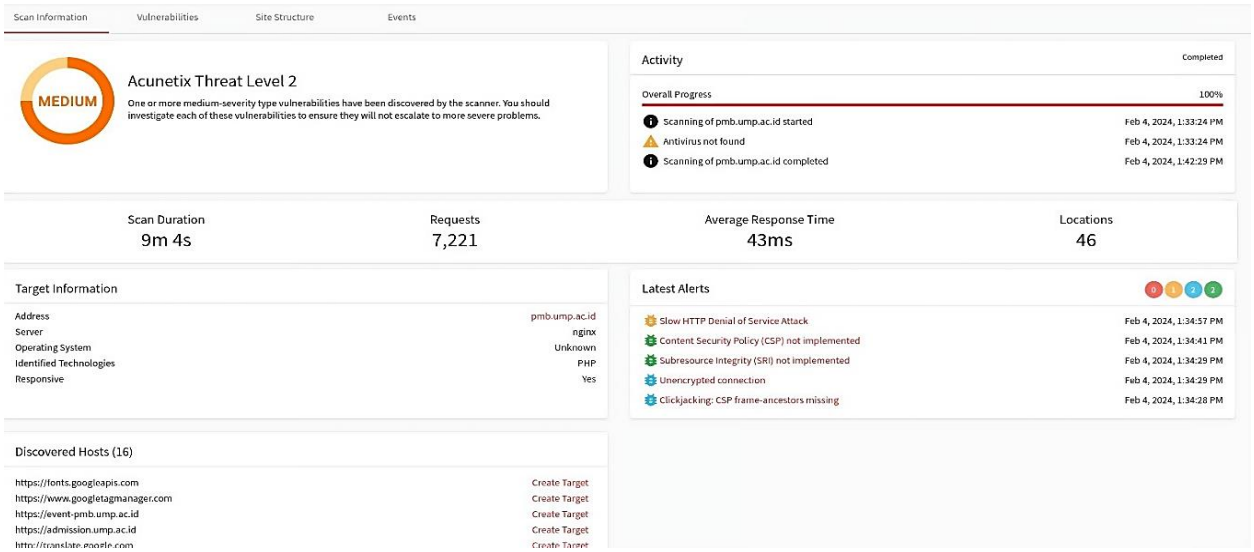
TIN: Terapan Informatika Nusantara
Vol 4, No 11, April 2024, page 698-708
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v4i11.5060

Tabel 2. Hasil *Footprinting* dan *Information Gathering*

No	*Tools Footprinting*	Informasi yang ditemukan target
1.	Zenmap	*Operating system (OS) version* Port-port yang terbuka *Traceroute* Topologi jaringan *Service* pada server dan *version*
2	Dnsdumpster	Nama domain Lokasi server Alamat IP *Server Software* Sub domain

3.1.3 Pengujian *vulnerability scanning*

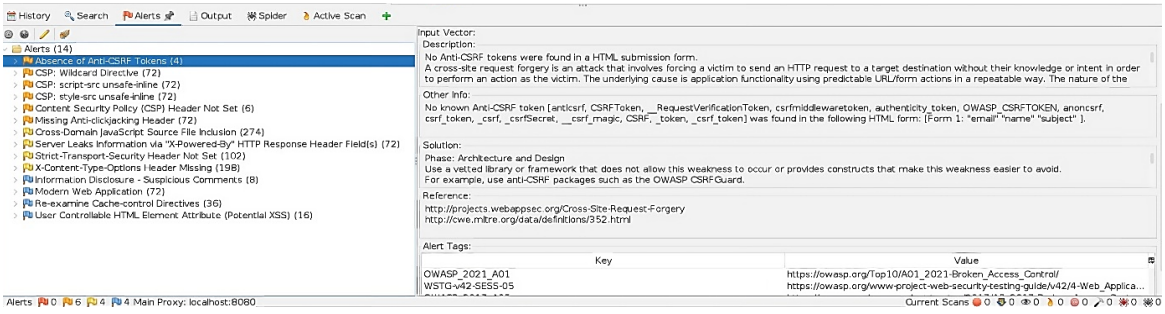
Teknik *Vulnerability scanning* merupakan proses untuk mendapatkan informasi celah keamanan terhadap sistem informasi yaitu *website* pendaftaran mahasasiwa pmb.ump.ac.id dengan memanfaatkan alat-alat *vulnerability scanner* seperti owasp zap, acunetix, serta nikto. *Scanning vulnerability* yang dilakukan pertamakali yaitu *scanning* dengan acunetix. Peneliti munggunakan *tools* acunetix *vulnerability* untuk mencari celah keamanan pada website pendaftaran mahasiswa baru dan untuk melihat tingkat kerentanan keamanan website tersebut. Pengujian *vulnerability scanning* dapat dilihat pada gambar 4 dibawah ini:



Gambar 4. *Scanning acunetix*

Dari hasil *scanning* yang dilakukan, *website* pendaftaran mahasiswa baru Universitas Muhammadiyah Purwokerto mendapatkan hasil *score* pada level 2, yang berati terdapat satu atau lebih kerentanan keamanan dengan jenis keparahan menenah telah ditemukan. Durasi *scan* yaitu 9 menit 4 detik. Pada hasil *vulnerability scanning* ini terdapat 5 *alert* atau celah keamanan yang diperoleh, yang terdiri dari 1 pada *level medium*, 2 *level low*, 3 *level informational*

Seusai melakukan *scanning vulnerability* dengan menggunakan *tools* acunetix, maka proses selanjutnya adalah *scanning vulnerability* owasp zap. Proses *vulnerability* dengan berbagai *tools vulnerability* ini dilakukan agar hasil dari suatu alat dapat divalidasi dikonfirmasi oleh celah keamanan yang diperoleh dari *tools* tersebut. *Scanning vulnerability* owasp zap dapat dilihat pada gambar 5:



Gambar 5. *Scanning* OWASP ZAP

TIN: Terapan Informatika Nusantara
Vol 4, No 11, April 2024, page 698-708
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v4i11.5060

Zed Attack Proxy atau biasa disebut OWASP ZAP adalah alat sumber terbuka, dikembangkan oleh OWASP guna melakukan tes penetrasi terhadap aplikasi web. Saat melakukan *scanning* ini dapat membantu mengidentifikasi dan mengatasi kerentenan keamanan pada aplikasi web. *Vulnerability scanning* terhadap website pendafataran mahasiswa baru Universitas Muhammadiyah Purwokerto menggunakan owasp zap telah menemukan 14 *alert* atau celah keamanan yang diperoleh, yang terdiri dari 6 pada *level medium*, 4 *level low*, dan 4 *level informational*.

Setelah melakukan *vulnerability scanning* dengan owasp zap, maka dilanjutkan dengan *scanning vulnerability* menggunakan nikto. Nikto adalah sebuah alat sumber terbuka yang digunakan untuk melakukan pemeindaian kerentanan terhadap server web. *Vulnerability scanning* nikto dapat dilihat pada gambar 6:

Gambar 6. *Scanning* Nikto

Scanning dengan menggunakan nikto dapat mendeteksi berbagai kerentanan keamanan pada server web, termasuk kerentanan dengan konfigurasi server, skrip yang tidak aman, dan kerentanan terhadap serangan lain. *Scanning* nikto ditemukan 2 *alert* yang terdiri dari 1 *level mediun* dan 1 *level low.*

3.1.4 Hasil pengujian dengan teknik *vulnerability scanning*

Langkah terakhir melakukan *vulnerability assessment* adalah *result.* Dari hasil pengujian teknik *vulnerability scanning website* pendaftaran mahasiswa baru Universitas Muhammadiyah Purwokerto memiliki kerentanan yang dimiliki. Berikut hasil beberapa pengujian yang disajikan pada tabel 3 dibawah ini:

Tabel 3. Hasil *Vunerability Scanning*

No	*Vulnerability Scanning*	*Alert*	*Risk Assesment*	Rekomendasi
1.	Acunetix	Slow HTTP Denial Of Service Attack	Medium	a. Menggunakan hardware balance b. Mengaktifkan konfigurasi mod_antiloris dan mod_reqtimeout
		Client Security Policy (CSP) not implemented	Informational	a. Implementasi Client Security Policy (CSP)
		Clickjacking: CSP frame-ancestors missing	Low	a. Menggunakan CSP frame ancestors b. Menggunakan X Frame Options
		Uncroted Connection	Low	a. Mengamankan koneksi dengan menggunakan protocol seperti HTTPS
		Subresource Integrity (SRI) not implemented	Informational	a. Menggunakan SRI Hash Generator
2.	OWASP Zap	Absence Anti-CSRF Tokens	Medium	a. Menggunakan anti CSRF
		CSP: Wildcard Directive	Medium	a. Mengkonfigurasi header CSP dengan lebih spesifik, menghindari penggunaan wildcard
		CSP: Script-src unsafe-inline	Medium	a. Memastikan web server, aplikasi server, load balancer mengkonfigurasi Content Security Policy header dengan benar
		CSP: Style-src unsafe-inline	Medium	a. Memastikan web server, aplikasi server, load balancer mengkonfigurasi Content Security Policy header dengan benar
		Content Security Policy (CSP)	Medium	a. Konfigurasi CSP header
		Missing Anti-Clicjacking header	Medium	a. Mengkonfigurasi Content Security (CSP) atau X Frame Options b. Implementasi direktif frame-ancestors dalam CSP
		Cross-Domain JavaScript Source File Inclusion	Low	a. Pastikan file JavaScript yang diunduh berasal dari sumber yang dapat dipercaya dan tidak dapat dimanipulasi oleh pengguna akhir
		Server Leaks Information “X-	Low	a. Pastikan konfigurasi web server, load balancer, aplikasi server telah diatu untuk

TIN: Terapan Informatika Nusantara
Vol 4, No 11, April 2024, page 698-708
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v4i11.5060

No	*Vulnerability Scanning*	*Alert*	*Risk Assesment*	Rekomendasi
		Powered-By" HTTP Response Header Fields(s)		menyembunyikan header "X-Powered-By"
		Strict-Transport-Security Header not set	Low	a. Pastikan pengaturan web server, aplikasi server, load balancer disesuaikan untuk menerapkan Strict Transport Security
		X-Content-Type-Options Header Missing	Low	a. Pastikan aplikasi/web server mengatur header jenis konten dengan benar dan 'nosniff'
		Information Disclosure-Suspicious Comments	Informational	a. Menghapus komentar yang memberikan informasi yang dapat membantu penyerang
		Modern Web Application	Informatioanl	Tidak ada
		Re-example cache-control directives	Informational	a. Pastikan HTTP control cache diatur dengan "no-cahce, no-stro, must-revalidate"
		User Controllable HTML Element Attribute (potential XSS)	Informational	a. Validasi semua masukan dan sanitasi keluaran sebelum menulis ke atribut HTML apapun
3.	Nikto	The anti-clickjacking X-Frame-Options header is not present	Medium	a. Menggunakan header X-Frame-Options
		The X-Content-Type-Option header is not set	Low	a. Menambahkan nilai "nonsnif" pada *Header X-Content-Type-Options*

3.1.5 Deskripsi kerentanan dan celah keamanan

Berdasarkan *vulnerability scanning* menggunakan alat pemindai kerentanan(acunetix, owasp zap, nikto) maka diperoleh 21 kerentanan dengan adanya 4 kerentanan yang sama, maka jumlah kerentanan yang ada adalah 17. Berikut merupakan penjelasan celah keamanan *website* setelah dilakukan pengujian dengan teknik *vulnerability scanning*:

a. *Slow HTTP Denial of Service Attack*
Memungkinkan terjadinya *Slow HTTP Denial of Service Attack*. Merupakan satu diantara bentuk teknik penyerangan DOS yang menyasar server HTTP. Teknik ini mengganggu layanan dengan cara membanjiri server sehingga menyebabkan antrian koneksi dengan permintaan yang lambat dan berlimpah menuju server web. Dampak dari kerentan ini sebuah mesin dapat mematikan web server dengan badwith minimal dan efek samping pada layanan dan port yang tidak terkait. Solusi dari permasalahan ini dapat menggunakan hardware balance. Kemampuan load balancing dalam mendistribusikan lalu lintas diseluruh server berguna untuk mempertahankan dari serangan DOS, karena ketika satu server kelebihan beban oleh serangan maka load balancing membantu merute ulang trafik dan mengalihkan ke server lain. Selain itu perl mengaktifkan konfigurasi mod_antiloris dan mod_reqtimeout untuk mengantisipasi.

b. *Content Security Policy (CSP) Header not set*
Merupakan Langkah keamanan yang dapat diambil pengembang web untuk melindungi aplikasi dari berbagai serangan, terutama *Cross-Site Scripting (XSS)*.

c. *Missing Anti-Clickjacing Header*
Ditemukan bahwa pada sebuah web atau situs, header anti *clicjacking* yang diperlukan tidak ada atau tidak diatur dengan benar. Solusi dari permasalahan ini adalah mengkonfigurasi *Content Security Policy (CSP)* atau *X Frame Options* dan meng-implementasi sirektif frame-ancestors dalam CSP.

d. *Uncrypted Connection*
Uncrypted Connection (koneksi tanpa enkripsi) menunjukkan bahwa sebuah web atau aplikasi terdeteksi koneksi antara pengguna dan server tidak dienkripsi. Koneksi tanpa enkripsi meningkatkan resiko keamanan karena informasi sensitive seperti data pribadi dapat terekspose dan dicuri dari pihak yang tidak memegang tanggung jawab. Untuk mengatasi kerentanan ini maka direkomendasikan menggunakan protocol enkripsi seperti HTTPS.

e. *Subresource Integrity (SRI) not implemented*
SRI adalah fitur keamanan yang memungkinkan browser memverifikasi bahwa sumberdaya pihak ketiga yang mereka ambil, dikirimkan tanpa manipulasi terduga. Fitur ini bekerja dengan mengizinkan pengembang untuk memberikan hash kriptografi yang harus cocok dengan file yang diambil.

f. *Absence of Anti-Cross Request Forgery (CSRF) Tokens*
Mengindikasikan bahwa aplikasi web rentan terhadap serangan *Cross-Site Request Forgery (CSRF)* karena tidak ada penggunaan token anti-csrf. Serangan pemalsuan permintaan lintas situs (CSRF) terjadi ketika situs web, email,

TIN: Terapan Informatika Nusantara
Vol 4, No 11, April 2024, page 698-708
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v4i11.5060

blog, pesan atau program berbahaya menipu browser web pengguna yang di autentikasi agar melakukan Tindakan yang tidak diinginkan disitus terpercaya. Menggunakan anti csrf dapat mengatasi kerentanan ini.

g. *CSP:Wildcard Directive*
Hasil dari scan adalah menunjukkan bahwa kebijakan CSP pada web menggunakan wildcard secara berlebihan atau tidak tepat. Penggunaan wildcard yang tidak terbatas dapat meninggalkan celah keamanan dan memungkinan serangan web terkait, untuk kerentanan ini maka direkomendasikan mengkonfigurasi header CSP dengan lebih spesifik, menghindari pengguanaan wildcard.

h. *CSP: Sript-src unsafe-iniline*
Menunjukkan bahwa CSP pada suatu aplikasi web memperbolehkan pengguna skrip Java Script langsung didalam elemen HTML (*inline script)* dengan menggunakan '*unsafe-inline*'. Hal ini memudahkan serangan XSS. Rekomendasi untuk kerentanan ini yaitu memastikan web server, aplikasi server *load balancer* mengkonfigurasi *Content Security Policy* dengan benar.

i. *Cross-Domain Java Script Source Fire Inclusion*
Hasil *scanning* menyatakan bahwa terdapat halaman yang menyatakan satu atau lebih file skrip dari domain pihak ketiga, untuk mangatasi kerentanan ini maka perlu memastikan file sumber Java script dimuat hanya dari sumber terpercaya dan sumber tersebut tidak dapat dikontrol oleh pengguna lain.

j. *Server Leaks Inforamation "X-Powered-By"HTTP*
Hasil menunjukkan bahwa server web/aplikasi mengungkapkan informasi melalui satu atau lebih header HTTP "*X-Powered-By*". Hal ini dapat menjadi resiko keamanan karean memberikan potensi petunjuk kepada penyerang tentang infrastruktur server yang dapat dieksploitasi. Pastikan bahwa web server, *application server, load balancer* disetel supaya menyembunyikan *header "X-Powered-By".*

k. *Stritct-Transport-Security Header Not Set*
Merupakan mekanisme kebijakan keamanan web Dimana server menyatakan bahawa agen pengguna yang mematuhi harus berinteraksi dengannya hanya menggunakan koneksi HTTPS yang aman.

l. *X-Content-Type-Options Header Missing*
Merupakan pengaturan pada header HTTP untuk melindungi web browser dari serangan MIME-snif yaitu dengan cara mempertahankan tipe konten pada aplikasi.

m. *CSP: style-src unsafe-inline*
Menunjukkan bahwa CSP pada suatu aplikasi web memperbolehkan pengguna *style* langsung didalam elemen HTML (*inline)* dengan menggunakan '*unsafe-inline*'. Hal ini memudahkan serangan XSS. Rekomendasi untuk kerentanan ini yaitu memastikan web server, aplikasi server *load balancer* mengkonfigurasi *Content Security Policy* dengan benar.

n. *Information Disclosure-Suspicious Comments*
Merujuk pada kode sumber atau halaman web terdapat komentar yang mencangkup informasi yang seharusnya tidak terbuka untuk public atau dimanfaatkan oleh pihak yang tidak berwenang.

o. *Modern Web Application*
Hanya berupa infomasional sehingga tidak diperlukan Tindakan lanjut.

p. *Re-examine Cache-control Directives*
Hasil menunjukkan bahwa *header* control *cache* belum di setel dengan benar. *Cache-control* adalah bagian dari *header HTTP* yang mengontrol sejauh mana di *cahce* oleh browser atau proxy server.

q. *User Conttrollable HTML Element Attribute*
Parameter string queri dan data post intuk mengidentifikasi Dimana nilai atribut HMTL terntentu dikontrol.

4. KESIMPULAN

Keamanan informasi merupakan hal yang harus diperhatikan bagi setiap instansi atau organisasi agar terhindar dari gangguan atau tindakan kejahatan. Peneliti dahulu menyatakan bahwa untuk mengidentifikasi celah keamanan pada sebuah sistem website, metode *vulnerability assessment* dapat digunakan. *Vulnerability assessment* merupakan langkah untuk mendefinisi, mengenali, dan mengetahui kerentanan dalam sistem komputer, aplikasi, dan jaringan infrastruktur. Proses ini memberikan organisasi evaluasi yang terperinci dengan pemahaman, kesadaran, dan informasi risiko yang diperlukan untuk memahami ancaman yang mungkin dihadapi dan dapat menanggapi secara efektif. Alat otomatis untuk menguji keamanan jaringan, seperti pemindaian biasanya digunakan dalam proses evaluasi kelemahan untuk mengidentifikasi ancaman dan risiko yang ditimbulkannya. Penelitian ini penulis menggunakan metode *vulnerability assessment*, dengan tujuan untuk mencari kerentanan dan celah keamanan terhadap *website* pendaftaran mahasiswa baru Universitas Muhammadiyah Purwokerto, dengan menggunakan *tools vulnerability* (acunetix, owasp zap, dan nikto). Beberapa hal yang dapat disimpulkan dari hasil penelitian ini yaitu, ditemukannya celah kerentanan keamanan pada situs web pendaftaran mahasiswa baru Universitas Muhammadiyah Purwokerto dengan menggunakan alat pindai kerentanan (acunetix, owasp zap, dan nikto) termasuk diantaranya 8 *risk level medium* seperti *Slow HTTP Denial Of Service Attack,Absence Anti-CSRF Tokens, CSP: Wildcard Directive, CSP: Script-src unsafe-inline, CSP: Style-src unsafe-inline, Content Security Policy (CSP), Missing Anti-Clicjacking header, The anti-clickjacking X-Frame-Options header is not present, 7 risk level low* yaitu *Clickjacking: CSP frame-ancestors missing, Uncroted Connection, Cross-*


TIN: Terapan Informatika Nusantara
Vol 4, No 11, April 2024, page 698-708
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v4i11.5060

Domain JavaScript Source File Inclusion, Server Leaks Information "X-Powered-By" HTTP Response Header Fields(s), Strict-Transport-Security Header not set, X-Content-Type-Options Header Missing, dan *The X-Content-Type-Option header is not set, 6 risk level informational* yaitu *User Controllable HTML Element Attribute (potential XSS), Modern Web Application, Re-example cache-control directives, Information Disclosure-Suspicious Comments, Subresource Integrity (SRI) not implemented, Client Security Policy (CSP) not implemented*. Berdasarkan hasil analisa celah keamanan web pendaftaran mahasiswa baru Universitas Muhammadiyah Purwokerto tingkat resiko dari kerentanan yang ditemukan adalah medium. Kerentanan dengan tingkat medium seringkali memerlukan tindakan perbaikan segera. Peneliti telah memberikan beberapa rekomendasi untuk mengatasi terkait temuan celah keamanan yang dapat digunakan.

REFERENCES

Adawiyyah, R., Fauzi, A., Indriyanah, A., Safitri, A., Nabila, E. P., Maidani, M., & Nurul, S. (2023). Pengaruh Keamanan Informasi dan Perkembangan Teknologi di Era Revolusi 4.0 Terhadap Kinerja Perusahaan (Literature Review Manajemen Kinerja). *JIM (Jurnal Ilmu Multidispilin)*, *2*(1), 2829–4599. https://creativecommons.org/licenses/by/4.0/

Alcianno, G. (2020). Sejarah dan Perkembangan Internet Di Indonesia Alcianno Ghobadi Gani, ST. *Jurnal Mitra Manajemen*, *5*(Cmc), 68–71.

Aulianisa, S. S., & Indirwan, I. (2020). Critical Review of The Urgency of Strenghthening The Implementation of Cyber Security and Resilience in Indonesia. *Lesrev (Lex Scientia Law Review)*, *4*(1), 33–48.

Badan Siber dan Sandi Negara. (2022). LANSKAP KEAMANAN SIBER INDONESIA 2022. In *Badan Siber dan Sandi Negara* (pp. 1–97).

Firmansyah, M. D., & Herman, H. (2023). Perancangan Web E- Commerce Berbasis Website pada Toko Ida Shoes. *Journal of Information System and Technology*, *4*(1), 361–372. https://doi.org/10.37253/joint.v4i1.6330

Hansen, R., & Panggabean, J. (2023). Memetakan Dinamika Kecenderungan Kreativitas Anak Gamers. *INNOVATIVE: Journal Of Social Science Research*, *3*(5), 3690–3703.

Harahap, P., & Zufria, I. (2024). Analisis Keamanan Pada Website UPM SAINTEK UIN- SU Medan Menggunakan Metode Vulnerability Assesment. *COSMIC JURNAL TEKNIK*, *2*(1), 10–20.

Hasanah, N. (2020). Analisis Website Pandawa Dengan Metode Webqual Info Artikel Abstrak. *Jurnal Penelitian Dan Pengabdian Kepada Masyarakat UNSIQ*, *7*(3), 260–265. http://pandawa.fastikom-unsiq.ac.id

Iin Nuraeniah, Muhamad Fatchan, A. S. (2024). Sistem Informasi Penyewaan Dump Truck Berbasis Website Menggunakan Metode Prototype. *Remik*, *8*(1), 176–185.

Karyati, A. (2024). Pemanfaatan Website Pembelajaran Bahasa Jepang dalam Meningkatkan Kemandirian Belajar Siswa. *AKSARA: Jurnal Ilmu Pendidikan Nonformal*, *10*(1), 75–90. http://ejurnal.pps.ung.ac.id/index.php/Aksara

Keriapy, F., Giban, Y., & Giban, T. (2022). Spiritualitas dalam Ruang Cyber (Cyberspace): Makhluk Digitalis sekaligus Spiritualis. *Tumou Tou*, *9*(2), 122–130. https://doi.org/110.51667/tt.v9i2.851

Kestina, L., & Nurcahyo, G. W. (2023). Penanganan Celah Keamanan Website dengan Ethical Hacking dan Issaf Menggunakan Acunetix Vulnerability (Studi Kasus di Bkpsdmd Kabupaten Kerinci). *INNOVATIVE: Journal Of Social Science Research*, *3*(4), 9192–9203.

Kustiawan, W., Harahap, D. K., Jannah, N. A., Sinaga, W. A., Safika, N., Lubis, H. A., & Al Barry, A. A. (2022). Media Online Dan Perkembangannya. *Maktabatum: Jurnal Perpustakaan Dan Informasi*, *Vol. 02*, *N*(01), 12. www.waspada.co.id,

Laksmiati, D. (2023). Vulnerability Assessment with Network-Based Scanner Method for Improving Website Security. *Journal of Computer Networks, Architecture and High Performance Computing*, *5*(1), 38–45. https://doi.org/10.47709/cnahpc.v5i1.1991

Lestari, Y. D., Zen, M., Rizal, C., & Fachri, B. (2022). Pelatihan Aplikasi Paket Niaga dan Internet di Cafetaria Tepi Kolam Kawasan Bukit Lawang Kabupaten Langkat , Sumatera Utara. *Jurnal Pengabdian Masyarakat (JAPAMAS)*, *1*(1), 38–47.

Luthfansa, Z. M., & Rosiani, U. D. (2021). Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet. *Journal of Information Engineering and Educational Technology*, *5*(1), 34–39. https://doi.org/10.26740/jieet.v5n1.p34-39

Maharani, D., Helmiah, F., & Rahmadani, N. (2021). Penyuluhan Manfaat Menggunakan Internet dan Website Pada Masa Pandemi Covid-19. *Abdiformatika: Jurnal Pengabdian Masyarakat Informatika*, *1*(1), 1–7. https://doi.org/10.25008/abdiformatika.v1i1.130

Muharrom, M., & Saktiansyah, A. (2023). Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVas. *International Journal of Engineering and Computer Science Applications (IJECSA)*, *2*(2), 51–58. https://doi.org/10.30812/ijecsa.v2i2.3297

Prasetya, F. (2023). Analisis Keamanan Situs Web Perpustakaan SMAN 3 Tambun Selatan Menggunakan Metode Vulnerability Assessment. *Jurnal Sains Dan Informatika*, *9*(1), 67–76. https://doi.org/10.34128/jsi.v9i1.488

Purba, N., Yahya, M., & Nurbaiti. (2021). Revolusi Industri 4.0 : Peran Teknologi Dalam Eksistensi Penguasaan Bisnis Dan Implementasinya. *Jurnal Perilaku Dan Strategi Bisnis*, *9*(2), 91–98.

Riadi, I., Yudhana, A., & W, Y. (2020). Analisis Keamanan Website Open Journal System Menggunakan Metode

TIN: Terapan Informatika Nusantara
Vol 4, No 11, April 2024, page 698-708
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v4i11.5060

Vulnerability Assessment. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *7*(4), 853–860. https://doi.org/10.25126/jtiik.2020701928

Rizkayanti, T., & Yunanri, W. (2023). ANALISIS KEAMANAN WEBSITE SISTEM INFORMASI ADMINISTRASI KEPENDUDUKAN MENGGUNAKAN METODE VULNERABILITY ASSESMENT. *JURTIKOM (Jurnal Teknologi Informatika Dan Komputer)*, *1*(1), 1–9.

Rohim, A., & Setiyani, L. (2023). Analisis Celah Keamanan E-LearningPerguruan Tinggi Menggunakan Vulnerability Assessment. *Jipakif*, *1*(1), 1–10.

Saputra, M. W. A., Ashari, S. A., & Larosa, E. (2024). Keamanan Data Sistem Informasi Akademik ITEkes Mahardika: Penerapan Sistem Pencadangan Basis Data dengan Enkripsi AES. *INVERTED: Journal of Information Technology Education*, *4*(1).

Saraswati, E., Gulo, W. A., Praditya, R. M., Ilham, D. M., & Wibowo, A. (2024). Pengembangan Sistem Penjualan Usaha Mikro Kecil Menengah (UMKM) Berbasis Web Menggunakan ODOO. *JAMASTIKA*, *3*(1), 4–6.

Siber, B., & Sandi, D. A. N. (2022). STRATEGI INDONESIA MEMBENTUK CYBER SECURITY DALAM MENGHADAPI ANCAMAN CYBER CRIME MELALUI. *Jurnal Dinamika Global*, *7*(2), 291–312.

Sunanta, U. K., & Wulandari, A. (2023). Perancangan Konten Marketing Di Media Sosial Instagram Dalam Akun @Merajut_Asa_ Pada Umkm Kampoeng Radjoet Tahun 2023. *E-Proceeding of Applied Science*, *9*(6), 2984.

Syafaat, A., & Subang, K. U. (2024). IDENTIFIKASI KERENTANAN KEAMANAN PADA WEBSITE FAKULTAS ILMU KOMPUTER UNIVERSITAS SUBANG MENGGUNAKAN METODOLOGI OWASP. *E-Journal*, *11*(1), 84–99. http://ejournal.unsub.ac.id/index.php/Fasilkom

Taryana, Y., & Nono, H. (2023). ANALISIS KEAMANAN WEBSITE BPJS KESEHATAN MENGGUNAKAN METODE VULNERABILITY ASESEMENT. *Journal of Informatica*, *8*(1), 31–37.

Ushud, A. A. A., Novita, I., & Juliasari, N. (2021). Pelatihan Pemanfaatan CMS Untuk Pembuatan Website Bagi OrangTua Siswa Sekolah Alam Tangerang. *JAM-TEKNO (Jurnal Pengabdian Kepada Masyarakat TEKNO)*, *2*(1), 20–25.

Wahyudin, W., Kuswara, H., Resti, R., & Dalis, S. (2024). Metode Vulnerability Assesment Dalam Pengujian Kinerja Sistem Keamanan Website Points of Sales. *Computer Science (CO-SCIENCE)*, *4*(1), 44–52. https://doi.org/10.31294/coscience.v4i1.2978